

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri**FILED**

JAN -6 2017

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

TWITTER ACCOUNTS 748794737390260224 AND
782409406596067333 THAT ARE STORED AT PREMISES
CONTROLLED BY TWITTER

Case No. 4:17 MJ 1028 JMB

APPLICATION FOR A SEARCH WARRANT

I, Kyle Storm, a federal law enforcement officer or an attorney for the government
request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

TWITTER ACCOUNTS 748794737390260224 AND 782409406596067333 THAT ARE STORED AT PREMISES CONTROLLED BY TWITTER

located in the Northern District of California, there is now concealed

See Attachments A&B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. Section 1028
 18 U.S.C. Section 1028A
 18 U.S.C. Section 1030
 18 U.S.C. Section 1343

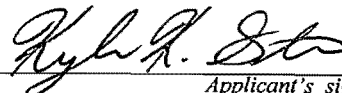
Offense Description

Identity Theft
 Aggravated Identity Theft
 Computer Intrusion
 Wire Fraud

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



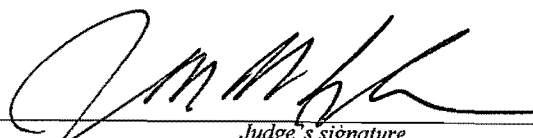
Applicant's signature

Special Agent Kyle Storm
Federal Bureau of Investigation

Printed name and title

Sworn to before me and signed in my presence.

Date:

1/7/17City and state: St. Louis, MO

Judge's signature

Honorable John M. Bodenhausen, U.S. Magistrate Judge

Printed name and title

AUSA: GWENDOLYN CARROLL

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
TWITTER ACCOUNTS 748794737390260224
AND 782409406596067333 THAT ARE STORED
AT PREMISES CONTROLLED BY TWITTER

Case No. 4:17 MJ 1028 JMB

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Kyle Storm, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Twitter account that is stored at premises owned, maintained, controlled, or operated by Twitter, a social-networking company headquartered in San Francisco, CA. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Twitter to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Twitter account.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since May 2016. I am currently assigned to the St. Louis Field Office of the FBI, assigned to full-time investigations of computer crimes with specific responsibility for criminal computer intrusions. Prior to my current assignment, from July 2014 to May 2016, I was a Staff Operations Specialist assigned to a cyber-squad specializing in cyber-criminal investigations. Through my training and experience as a special agent, I am familiar with investigations

involving individuals who execute computer intrusions, including the execution of search warrants on computers and email accounts.

3. I have also participated in the execution of many state, local, and federal search warrants, a number of which involved Computer Intrusion as detailed by Section 1030 of Title 18, United States Code. I am an "investigative or law enforcement officer" of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1028 (identity theft), 1028A (aggravated identity theft), 1030 (computer intrusion) and 1343 (wire fraud), and conspiracy to commit such offenses, have been committed by unknown persons. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

PROBABLE CAUSE

6. On or about May 3, 2016, a user of the Onion Router (“TOR”)¹ forum “Hell Reloaded” offered to sell compromised Remote Desktop Protocol (RDP) credentials to unidentified clinics in the central United States. As proof of the compromise the user posted obfuscated screenshots of a Missouri driver’s license and Commerce Bank Visa card belonging to a customer of the clinic.

- a. Hell Reloaded was an online forum accessible through TOR and required an invitation for access.
- b. RDP is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

7. The user also advertised logins to provider portals for seventeen health insurance companies. These portals would provide access to Personally Identifiable Information (PII) for individuals covered by those insurance companies. The provider portals were for the following insurance companies:

- i. Aetna
- ii. AIM
- iii. Availity

¹ Tor is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name “The Onion Router”. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than seven thousand relays to conceal a user’s location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the user.

- iv. BCBS
- v. Cigna
- vi. GHP/Coventry
- vii. Humana
- viii. Medicaid
- ix. NIA
- x. Noridian
- xi. One Call
- xii. Optum
- xiii. Payspan
- xiv. PNC
- xv. Tricare
- xvi. UHC
- xvii. UMR

8. The user claimed to have access to a few United States Hospitals as well, in total had access to 3TB of data.

9. Based on the information provided by the user it was determined the screen shots posted used “medtech” software, and showed a computer name of “MIDORTH-SVR-02”.

10. “MOC,” a health care provider company located in Farmington, MO (“the Company”), was notified and provided with the screen shot identifiers. The Company confirmed the software and computer name belonged to them.

11. The Company believed the compromise occurred through a remote access computer, possibly through the computers of a medical records company (“QMR”). QMR

completed insurance billings on behalf of the Company. QMR had authority by the Company to RDP into their network.

12. On or about June 2, 2016, the Company provided an individual by the name of Marco Weebler contacted their office. Marco Weebler initially acted as a potential patient and wanted to meet with a doctor associated with The Company. Marco Weebler provided his email address as marco.weebler72@gmail.com.

13. On or about June 9, 2016, through email address marco.weebler72@gmail.com the following correspondence occurred between Marco Weebler and the Company.

- a. "I do hope this is being taken seriously by [The Company]. I have not heard from him yet."

14. On or about June 10, 2016, through email address marco.weebler72@gmail.com the following correspondence occurred between Marco Weebler and the Company.

- a. The Company received an email stating, "we will not be responding or viewing this email address anymore after this message to you. It is up to you, [the Company], to take the appropriate action and do what is right for you, your employees, and your company. This was not supposed to work out like this, but since you do not take us seriously, we are forced to move onto the next best thing....." ".....We hate to be the bearer of bad news, but [the Company] is ours now." ".....If you for some reason still aren't grasping what we are saying. We have hacked your network and we have everything, including your valuable electronic patient records." ".....you [the Company] will create an account with Coinbase (a U.S. based bitcoin exchange) for the purpose of purchasing a large volume of bitcoins to satisfy our demand." ".....you [the Company] will do this

until the address has been sent a total of 250 BTC.” “....you have untilJuly 8, 2016 to satisfy our demand.”

15. On or about June 27, 2016, a hacker who goes by the name “thedarkoverlord” provided images containing PII to “Deep Dot Web”.

- a. The dark web, or darknet refers to private networks built from connections between trusted peers using unconventional protocols. The Deep Dot Web is just one part of what is known as deep web, a vast network which is not indexed by search engines such as, Google and Bing.

16. The hacker posted they had access to databases from three different healthcare organizations. One database originated in Farmington, MO and contains 48,000 patient records. A second database from the Central/Midwest U.S.A contains 210,000 patient records. A third database from Georgia, U.S.A. had records on 397,000 patients.

17. The hacker posted one copy of each database is being sold on “TheRealDeal,” a dark web marketplace that provides anonymity to buyers and sellers.

USE OF TWITTER

18. On June 24, 2016, a preservation request was sent to Twitter for records associated with @TDOhack3r.

19. On July 13, 2016, legal process was served on Twitter for records associated with @TDOhack3r. On July 21, 2016, Twitter provided the results associated with account @TDOhack3r.

- a. The subscriber information for @TDOhack3r provided email address as marco.weebler72@gmail.com, screen name as TDOhack3r, and was created on July 1, 2016.

20. On or about July 10, 2016, a hacker who goes by the name “thedarkoverlord” sent an email to “POC” from an internal POC email address. The email claimed, “We are responsible for the largest and most devastating healthcare breaches of this year.” “.....Your network has been hacked. We have your patient records and your documents. We also made a quick tweet on your Twitter account and made you give us a follow. We’ve been inside every single computer on your network and every account. We have everything stored on Medflex. We have everything that you have.” “.....Unless you want us to leak everything to the public for all to see then you will pay us \$75,000 USD in bitcoins (BTC) to the following address.....by the 25th of July.....” “.....to incentivize you, you’ll find that your data is already for sale on the black market and we’re selling it for far less than \$75,000 USD. You will find a link to the listing if you view our recent activity from our Twitter “@tdohack3r.”

- a. The email to “POC” provided proof of being inside their network by providing, names, social security numbers, addresses, phone numbers, date of births, and email addresses. “POC” confirmed the names identified were patients of “POC”.
- b. The email to “POC” stated, “since we sent this from inside your network, you can reach us at: marco.weebler72@gmail.com.” Signed “Warmest Regards, thedarkoverlord, Professional Adversary, World Wide Web, LLC.”

21. On or about July 11, 2016, “POC”, a health care clinic located in St. Louis, MO provided that @TDOhack3r posted pictures of patients on the twitter account. POC confirmed the pictures were of POC patients.

22. On or about July 13, 2016, @TDOhack3r posted “the Company” from MOC was “named and shamed”.

23. On or about August 3, 2016, a search warrant was executed on Twitter for records associated with Twitter account @TDOhack3r.

24. On or about August 4, 2016, Twitter returned the requested records related to the search warrant executed on @TDOhack3r. The records returned were from Twitter account number 748794737390260224.

25. On or about December 14, 2016, an individual from Pre-Con Products (Victim 1) contacted the FBI Public Access Line to report a computer intrusion into their network. Victim 1 had received an email titled Extortion on December 13, 2016. The email informed him all of his files had been encrypted and gave payment instructions on how to have the files restored. The email indicated it originated from Thedarkoverlord Professional Adversary LLC. Victim 1 advised they had lost sales and marketing information, as well as, engineering drawings.

26. On or about December 17, 2016, @tdohack3r posted "Using a sledgehammer is one way to break up concrete, we prefer a different tool. Parting is such sweet sorrow. Pastebin.com/4D0YKjtf".

a. Victim 1 is a large producer of various concrete products.

27. On or about December 17, 2016, a user posted Pastebin.com/4D0YKjtf stating "This is thedarkoverlord (@tdohack3r) here to deliver a message. We've taken an interest in contractors who have worked with the United States military". The user later stated "Unsurprisingly, some of our new targets are taking the "we don't negotiate with terrorists" stance. We'd like to single out one of our targets in particular, Precon Products. Meet Precon Products (<http://www.preconproducts.com/>), they're a construction company who had their data stolen by us. They're located in the state of California and are known to work with the US Navy." The user later stated "We're going to give Precon Products the opportunity to stop the

bleeding and walk away from this with only a few scratches, an opportunity that these poor people weren't given. All they have to do is work with us, and we're looking forward to doing just that." A link to the website mega.nz was provided with Precon Product's stolen files available for access. The post was signed "Regards, thedarkoverlord Professional Adversary World Wide Web, LLC".

28. On or about December 21, 2016, a preservation letter was sent to Twitter for records associated with @TDOHack3r, account 748794737390260224. On or about December 23, 2016, Twitter responded to the preservation request stating "the username you provided does not match the UID you provided (748794737390260224). Please confirm the Twitter account that is the subject of your request."

29. On or about December 23, 2016, open source research indicated Twitter handle @tdohack3r was an active username. However, the twitter account number was 782409406596067333. The name displayed on the account was "thedarkoverlord". The new Twitter account number stated it had "Joined October 2016".

- a. It is likely that Twitter account 748794737390260224 was deactivated sometime in October 2016 and a new account, 782409406596067333, was created in its place utilizing the same Twitter handle, @tdohack3r, and display name, "thedarkoverlord".

30. On or about December 25, 2016, @tdohack3r posted "Any parties interested in source code classified as SECRET? Use it to get an edge over the US Navy and defense contractors! Emails included!"

31. On or about December 25, 2016, @tdohack3r posted “There aren’t many screeners during screener season this year. Someone should do something about that. Pastebin.com/6Pw7TxEp”.

32. On or about December 25, 2016, a user posted Pastebin.com/6Pw7TxEp stating “This is thedarkoverlord (tdohack3r) here to deliver a message. You may have already noticed we have tweeted about source code classified as SECRET and emails about the project(s) which were heisted from a contractor. We are taking open offers. In other news, we come bearing more companies and consequentially more data. We have not one but two companies to bring to the slaughterhouse.” The post listed G.S. Polymers Inc. (www.gspolymers.com) and DRI Title & Escrow (www.drititle) as the two companies. The user later stated “Like G.S. Polymers, DRI Title & Escrow exhibited the same behavior which, as you all know, is a big no-no in our book. And like G.S. Polymers, we are also releasing a small set of sample documents from their company and providing them the opportunity to come to their senses before they make a mistake that cannot be undone.” A link to the website mega.nz was provided for both G.S. Polymers and DRI Title & Escrow with their stolen files available for access. The post was signed “Regards, thedarkoverlord Professional Adversary World Wide Web, LLC”.

33. On or about December 27, 2016, a representative from “DRI” (Victim 2) contacted FBI St Louis stating they had received a series of emails from, jasonmelli@protonmail.com, by an individual using the moniker thedarkoverlord.

- a. On or about December 24, 2016, Victim 2 received an email from jasonmelli@protonmail.com that stated “Dear DRI Title & Escrow, This is usually where we would put some very witty introduction to leave a lasting impression and the set the tone for the rest of the letter, but we simply don’t care

enough because we are not very impressed with your company.”....”We are sure that by now you are wondering who we are. Allow us to introduce ourselves. We are thedarkoverlord. If you receive a message from us, that means you have been completely and thoroughly hacked by a group of creatures who are motivated only by their greed and are responsible for some of the most serious breaches of 2016.”....”We have successfully attacked your corporate infrastructure and have pillaged your network of valuable trade secrets, operations data and information, your entire customer and client related databases, and a treasure trove of extremely sensitive documents that could make the fraud community very happy, among other things.”....”Fine you say. They have all of our data, so what do we do? We have a few demands which you will satisfy to the letter unless you would like us to wreak havoc upon your company.” The email demanded payment of 120 bitcoins over a four-month period with the first payment being made by January 31, 2016. The email offered other options for payment. The email later stated “Along with the aforementioned documents, we’ve attached a small submission of various documents from different places in your network.” A link to the website mega.nz was provided with Victim 2’s stolen files available for access. The email was signed “Sincerely, thedarkoverlord Professional Adversary World Wide Web, LLC”.

- b. On or about December 25, 2026, Victim 2 received an email from jasonmelli@protonmail.com that stated “Hello, You have only a few hours left to reply to us before we have to escalate this situation. We suggest you make the right choice and work with us, otherwise you will suffer and be on the losing end

of this ordeal.” The email was signed “Regards, thedarkoverlord Professional Adversary World Wide Web, LLC”.

- c. On or about December 25, 2016, Victim 2 received an email from jasonmelli@protonmail.com that stated “Hello, We have started your first round of public punishment. We suggest you start cooperating or this will only heat up.” The email provided two links, <https://twitter.com/tdohack3r/status/813145161412804608>, and <http://pastebin.com/6Pw7TxEp>. The email was signed “Regards, thedarkoverlord Professional Adversary World Wide Web, LLC”.

TWITTER

34. Twitter owns and operates a free-access social-networking website of the same name that can be accessed at <http://www.twitter.com>. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users create and read 140-character messages called “Tweets,” and to restrict their “Tweets” to individuals whom they approve. These features are described in more detail below.

35. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

36. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user’s full name, e-mail

addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.

37. A Twitter user can post a personal photograph or image (also known as an "avatar") to his or her profile, and can also change the profile background or theme for his or her account page. In addition, Twitter users can post "bios" of 160 characters or fewer to their profile pages.

38. Twitter also keeps IP logs for each user. These logs contain information about the user's logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

39. As discussed above, Twitter users can use their Twitter accounts to post "Tweets" of 140 characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also "favorite," "retweet," or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a "mention" of the identified user. In the "Connect" tab for each account, Twitter provides the user with a list of other users who have "favorited" or "retweeted" the user's own Tweets, as well as a list of all Tweets that include the user's username (*i.e.*, a list of all "mentions" and "replies" for that username).

40. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services.

41. Twitter users can also opt to include location data in their Tweets, which will reveal the users' locations at the time they post each Tweet. This "Tweet With Location" function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data.

42. When Twitter users want to post a Tweet that includes a link to a website, they can use Twitter's link service, which converts the longer website link into a shortened link that begins with <http://t.co>. This link service measures how many times a link has been clicked.

43. A Twitter user can "follow" other Twitter users, which means subscribing to those users' Tweets and site updates. Each user profile page includes a list of the people who are following that user (*i.e.*, the user's "followers" list) and a list of people whom that user follows (*i.e.*, the user's "following" list). Twitter users can "unfollow" users whom they previously followed, and they can also adjust the privacy settings for their profile so that their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into "lists" that display on the right side of the user's home page on Twitter. Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

44. In addition to posting Tweets, a Twitter user can also send Direct Messages (DMs) to one of his or her followers. These messages are typically visible only to the sender and

the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter's database.

45. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user's mobile phone, and the user can also set up a "sleep time" during which Twitter updates will not be sent to the user's phone.

46. Twitter includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches.

47. Twitter users can connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Twitter profiles.

48. If a Twitter user does not want to interact with another user on Twitter, the first user can "block" the second user from following his or her account.

49. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

50. As explained herein, information stored in connection with a Twitter account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Twitter user’s account information, IP log, stored electronic communications, and other data retained by Twitter, can indicate who has used or controlled the Twitter account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, communications, “tweets” (status updates) and “tweeted” photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Twitter account at a relevant time. Further, Twitter account activity can show how and when the account was accessed or used. For example, as described herein, Twitter logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Twitter access, use, and events relating to the crime under investigation. Additionally, Twitter builds geo-location into some of its services. If enabled by the user, physical location is automatically added to “tweeted” communications. This geographic and timeline information may tend to either inculcate or exculpate the Twitter account owner. Last, Twitter account activity may provide relevant insight into the Twitter account owner’s state of mind as it relates to the offense under investigation. For example, information on the Twitter account may indicate the owner’s motive and intent to commit a crime (*e.g.*, information indicating a criminal

plan) or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

51. Therefore, the computers of Twitter are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Twitter, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

52. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Twitter to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

53. Based on the forgoing, I request that the Court issue the proposed search warrant.

54. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

55. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Twitter accounts 748794737390260224 and 782409406596067333 since August 3, 2016 to the present, that are stored at premises owned, maintained, controlled, or operated by Twitter, a company headquartered in San Francisco, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Twitter

To the extent that the information described in Attachment A is within the possession, custody, or control of Twitter, including any messages, records, files, logs, or information that have been deleted but are still available to Twitter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Twitter is required to disclose the following information to the government for each account listed in Attachment A:

- a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
- b. All past and current usernames, account passwords, and names associated with the account;
- c. The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;
- d. All IP logs and other documents showing the IP address, date, and time of each login to the account;
- e. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;
- f. All "Tweets" and Direct Messages sent, received, "favorited," or retweeted by the account, and all photographs or images included in those Tweets and Direct Messages;

- g. All information from the “Connect” tab for the account, including all lists of Twitter users who have favorited or retweeted Tweets posted by the account, as well as a list of all Tweets that include the username associated with the account (*i.e.*, “mentions” or “replies”);
- h. All photographs and images in the user gallery for the account;
- i. All location data associated with the account, including all information collected by the “Tweet With Location” service;
- j. All information about the account’s use of Twitter’s link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;
- k. All data and information that has been deleted by the user;
- l. A list of all of the people that the user follows on Twitter and all people who are following the user (*i.e.*, the user’s “following” list and “followers” list);
- m. A list of all users that the account has “unfollowed” or blocked;
- n. All “lists” created by the account;
- o. All information on the “Who to Follow” list for the account;
- p. All privacy and account settings;
- q. All records of Twitter searches performed by the account, including all past searches saved by the account;
- r. All information about connections between the account and third-party websites and applications;

- s. All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1028 (identity theft), 1028A (aggravated identity theft), 1030 (computer intrusion), and 1343 (wire fraud), and conspiracy to commit such offenses involving accounts 748794737390260224 and 782409406596067333 since August 3, 2016 to the present, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- a. Information or evidence relating to the intrusion and exfiltration of personally identifiable information.
- b. Information relating to the acquisition and location of online infrastructure that may be used in a network intrusion, including but not limited to domains, servers, IP addresses and other e-mail addresses, and the source(s) of funding used to acquire such infrastructure;
- c. Evidence indicating how and when the Twitter account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Twitter account owner;
- d. Evidence indicating the Twitter account owner's state of mind as it relates to the crime under investigation;

- e. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- f. Information that could lead to the identification of co-conspirators and their whereabouts;
- g. Information relating to the use or other disposition of the fraudulently acquired personally identifiable information;
- h. Information relating to any criminal proceeds, including the disposition of such proceeds, resulting from the intrusion; and
- i. Information that could lead to the identification of victims of the intrusion.
- j. The identity of the person(s) who communicated with the user ID about matters relating to computer intrusion and identify theft, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS
PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Twitter, and my official title is _____. I am a custodian of records for Twitter. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Twitter, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Twitter; and
- c. such records were made by Twitter as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature